Martin Hellman popsal první time-memory tradeoff útok na blokové šifry. Jedná se o útok s volbou otevřeného textu, ve kterém útočník předpočítá velké množství dat k jedné blokové šifře a pak jej může opakovaně využít k útoku na danou šifru. Vylepšení, které navrhl Ron Rivest, zrychluje útok tím, že snižuje počet čtení z disku. Další pozměnění původního útoku s názvem duhové tabulky zrychluje útok ještě více a přináší další výhody. Time-memory tradeoff útoky mohou být využity také na proudové šifry jako útoky se znalostí otevřeného textu. Tato bakalářská práce popisuje původní útok, jeho vylepšení a úpravu pro proudové šifry. Jako příklad je shrnut útok na konkrétní proudovou šifru A5/1. Je navržen nový time-memory tradeoff útok na blokové šifry nazývaný r-barevné duhy. Tento nový útok je úpravou Hellmanova útoku a sdílí společné prvky s duhovými tabulkami. Vlastnosti těchto tří útoků jsou porovnány a závěrem je, že pro určité blokové šifry, může být navržený útok nejefektivnější.